



⑮ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ Off nlegungsschrift
⑩ DE 44 26 428 A 1

⑤① Int. Cl.⁸:
G 07 C 9/00
G 07 F 19/00
H 04 M 1/66

⑳ Aktenzeich n: P 44 26 428.3
㉔ Anmeldetag: 26. 7. 94
㉕ Offenlegungstag: 23. 11. 95

DE 44 26 428 A 1

③① Unionspriorität: ③② ③③ ③①
19.05.94 CN 94105095 30.06.94 GB 9413204

⑦① Anmelder:
Wong, Kam-Fu, Shatin, Hongkong, HK

⑦④ Vertreter:
Patent- und Rechtsanwälte BOEHMERT &
BOEHMERT, NORDEMANN UND PARTNER, 28209
Bremen

⑦② Erfinder:
gleich Anmelder

⑤④ Sicherheitssystem

⑤⑦ Ein Sicherheitssystem zum Verhindern von unzulässigen Transaktionen mit einer den Vorgang bearbeitenden Einrichtung zum Registrieren einer versuchten Transaktion und Mitteln zum Inkenntnissetzen einer zur Ausführung der Transaktion berechtigten Person von der versuchten Transaktion.

DE 44 26 428 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 09. 95 508 047/480

15/29

Die Erfindung betrifft ein Sicherheitssystem und insbesondere ein Sicherheitssystem, mit dem ein berechtigter Eigentümer Andere an der Verwendung seiner gestohlenen Kreditkarte oder einem gestohlenen Mobiltelefon hindern kann.

In der modernen Gesellschaft erfolgen mehr und mehr Transaktionen mittels sofortiger unbarer Zahlungen. Wenn jemand einkaufen geht, ein privates Mobiltelefon oder aber ein Zellulartelefon für ein Ortsgespräch, ein Ferngespräch oder aber ein Auslandsgespräch verwendet, wird die Rechnung monatlich oder vierteljährlich bezahlt. Es ist weiter üblich, verschiedene als Zahlungsmittel dienende Karten wie Kreditkarten, Guthabenkarten, Clubkarten, Telefonkarten oder dergleichen zu verwenden. Bei diesen Transaktionen erfolgt die Belastung des Verwenders entweder sofort oder aber es erfolgt eine monatliche oder vierteljährliche Abrechnung. Die verschiedenen Transaktionen schließen auch das Essen in einem Restaurant, die Hotelübernachtung, die Beherbergung, den Kauf von Flugtickets oder Zugfahrkarten ein. Nach einer Zeitdauer werden die Rechnungen durch direkte Zahlung, Scheckzahlung oder dergleichen beglichen.

Es ist auch üblich, persönliche Sicherheitscodes, nämlich persönliche Identifikationszahlen (PINS) zu verwenden, um eine Transaktion zu autorisieren. Ein Telefon, ein Computer oder aber ein Kassensystem kann verwendet werden, um eine PIN einzugeben, durch die eine Transaktion autorisiert wird.

Wenn Kunden eine unbare Sofortzahlung verwenden, um Rechnungen oder dergleichen zu bezahlen, ist es nicht erforderlich, daß diese erhebliche Mengen an Bargeld mit sich führen. Der Verwender hat so ein geringeres Risiko des Verlierens von Bargeld, er fühlt sich nicht aufgrund des Mitschüffens von Bargeld unwohl und hat geringeren Kontakt mit verschmutzten Banknoten, die von anderen Menschen berührt worden sind. Die sofortigen unbaren Zahlungen führen jedoch zu Problemen und Risiken. Transaktionen mit Kreditkarten und Zellulartelefonanrufen basieren auf moderner elektronischer Technologie, Computertechnologie und der Technologie einer Fernübertragung. Diese Technologien sind mit bekannten Sicherheitsverfahren schwer zu schützen. Kriminelle verwenden fortgeschrittene Technologien, um von Verwendern Kreditkarten oder deren Zellulartelefone zu stehlen und Informationen bezüglich der Geheimcodes und persönlichen Identifikationsziffern zu gewinnen, um falsche Transaktionen mit den Kreditkarten und den Zellulartelefonanrufen auszuführen. Die zunehmende Verwendung von unbaren sofortigen Zahlungen haben diese Probleme immens gesteigert.

Nachfolgend werden Beispiele von illegalen unbaren sofortigen Zahlungen beschrieben.

Wenn ein Mobiltelefon eines Verwenders verloren oder gestohlen ist, kann der Finder bzw. der Dieb die internen Charakteristika des Mobiltelefons wie ESN oder MIN kopieren, um damit widerrechtlich eine Reproduktion des Mobiltelefons herzustellen derart, daß alle weiteren Anrufe, die von dem Mobiltelefon aus durchgeführt werden, dem berechtigten Eigentümer des Telefons berechnet werden.

Wenn Kundenkarten wie Kreditkarten, Warenkarten oder dergleichen von einem Dieb gestohlen werden oder aber wenn die Information, die auf der Kreditkarte enthalten ist, von einem Dieb gestohlen wird und von

dieser widerrechtlich eine Karte produziert wird, können Händler oder Banken die gestohlene Kreditkarte oder die reproduzierte Kreditkarte akzeptieren, was zu Verlusten bei den Kunden oder aber bei den Banken führt. Berichte zeigen, daß gegenwärtig annähernd 20 Millionen Kreditkarten pro Jahr als verloren oder als gestohlen gemeldet werden. Der Geldverlust aufgrund des Mißbrauchs von Kreditkarten beläuft sich auf mehrere hundert Millionen US\$. Bisher gibt es keine Lösung für die genannten Probleme.

Es ist die Aufgabe der vorliegenden Erfindung, die oben genannten Probleme zu lösen oder zu mildern.

Erfindungsgemäß wird diese Aufgabe durch ein Sicherheitssystem zum Verhindern von unerlaubten Transaktionen gelöst, das eine Vorgangseinrichtung zum Registrieren des Versuchs einer Transaktion oder Kommunikationsmittel zum Benachrichtigen einer autorisierten Person, daß die Transaktion eine zugelassene Transaktion ist, aufweist.

Die vorliegende Erfindung schafft ein Verfahren zum Schützen von unbaren, sofortigen Zahlungstransaktionen. Auch wenn der wahre Eigentümer einer Kreditkarte und/oder eines Mobiltelefons keine Kenntnis davon hat, daß seine Karte und/oder sein Mobiltelefon gestohlen oder aber verlorengegangen ist, kann er unmittelbar wissen, wenn jemand die gestohlene Karte und/oder das Mobiltelefon verwendet, um eine unerlaubte Transaktion durchzuführen. Der wahre Eigentümer kann so dann entscheiden, ob die Transaktion legal oder illegal ist. Wenn die Transaktion illegal ist, kann eine sofortige Aktion unternommen werden, um die Bank, den Händler oder aber die Telefongesellschaft darüber zu informieren, daß die illegale Transaktion zu unterbinden ist, die Zahlung der Waren zurückzuweisen ist, die Verwendung der Kreditkarte zu stoppen oder aber die Verwendung des Mobiltelefons zu stoppen, so daß jedwede Verluste des wahren Eigentümers, der Bank oder des Händlers verringert oder auch ausgeschlossen sind. Das Verfahren nach der Erfindung wird so diese Art von gewerblichen Vergehen reduzieren oder eliminieren.

Zum besseren Verständnis der Erfindung werden Ausführungsbeispiele beispielhaft unter Bezugnahme auf die beiliegenden Zeichnungen erläutert. Dabei zeigt:

Fig. 1 eine Flußdarstellung eines Verfahrens der Verwendung eines Sicherheitssystems, das die vorliegende Erfindung verwirklicht;

Fig. 2 ein schematisches Blockdiagramm eines Sicherheitssystems, das die vorliegende Erfindung verwirklicht;

Fig. 3-1 und 3-2 schematische Darstellung der Adreßcodes, die in den Kontoempfängern gespeichert sind;

Fig. 4 eine schematische Blockdarstellung eines anderen Sicherheitssystems, welches die vorliegende Erfindung verwirklicht;

Fig. 5 eine schematische Blockdarstellung eines weiteren Sicherheitssystems, das die vorliegende Erfindung verwirklicht;

Fig. 6 ein schematisches Blockdiagramm eines Vorgangssignale verarbeitenden Computerzentrums zur Verwendung mit einem Sicherheitssystem, welches die vorliegende Erfindung verwirklicht;

Fig. 7 ein schematisches Blockdiagramm einer die Polizei informierenden Einheit zur Verwendung mit einem Sicherheitssystem, das die vorliegende Erfindung verwirklicht.

Fig. 1 zeigt ein Flußdiagramm, das die Schritte nach einem Verfahren der Verwendung eines Sicherheitssystems nach der Erfindung angibt. Wenn eine Person ein

Mobiltelefon oder aber ein Autotelefon verwendet, um einen Anruf zu tätigen oder aber jemand versucht, eine Transaktion unter Verwendung einer Kreditkarte auszuführen, findet eine unbare sofortige Zahlungstransaktion statt. Eine solche Transaktion wird im folgenden als "Vorgang" bezeichnet. Der Wahlvorgang des Mobiltelefons informiert ein rechnergestütztes Kontenführungssystem der Telefongesellschaft, die das Mobiltelefon betreibt, das das Mobiltelefon verwendet wird und beginnt zu rechnen um die Zeit, den Ort, den Abstand und die Kosten des Telefonanrufs aufzuzeichnen. Wenn jemand eine Kreditkarte verwendet, um eine Transaktion zu bewirken und die Kreditkarte von einer Einrichtung zum Auslesen einer Kreditkarte am Ort des Verkaufs gelesen wird, beginnt ein entsprechendes rechnergestütztes Kontenführungssystem in einer Bank oder dem Händler damit, die Transaktion auf der Karte aufzuzeichnen. Zu diesem Zeitpunkt erzeugt das rechnergestützte Kontenführungssystem beispielsweise bei der Bank ein Vorgangssignal. Das rechnergestützte Kontenführungssystem wertet aus der vorgesehenen Information den persönlichen Adreßcode des wahren Eigentümers der Kreditkarte bzw. des Telefons aus. Eine Ausgangeinrichtung in dem rechnergestützten Kontenführungssystem gibt ein Signal, das das Vorgangssignal beinhaltet, an eine Vorgangssignalübertragungsstation mittels Radioübermittlung, Telefonleitungen oder anderen Kommunikationsleitungen aus. Die Vorgangsübertragungsstation verarbeitet die empfangenen Signale und übersendet diese Signale über einen großen Bereich. Der wahre Eigentümer der Kreditkarte bzw. des Mobiltelefons trägt einen Kontenempfänger, der das übertragene Signal empfängt, einschließlich des Vorgangssignals, wodurch der wahre Eigentümer davon in Kenntnis gesetzt wird, daß ein Vorgang, der eine Transaktion angibt, von jemandem, der seine Kreditkarte oder sein Telefon verwendet, ausgeführt wird.

Der Kontenempfänger kann beispielsweise ein Display aufweisen, daß das Zeichen "B25" angibt, um anzuzeigen, daß die Karte des Eigentümers bei einer Transaktion mit dem Betrag von US 25 benutzt wird. Eine Angabe "STBJ" kann beispielsweise angeben, daß das Mobiltelefon des Verwenders dazu benutzt wird, mit Beijing zu telefonieren. Wenn der Eigentümer das Signal über den Kontenempfänger aufnimmt, kann der Eigentümer sofort entscheiden, ob der Vorgang rechtmäßig von ihm zugelassen ist oder aber unberechtigt von anderen ausgeführt wird. Beispielsweise wenn das zur Ausführung des Anrufs verwendete Telefon eine widerrechtliche Reproduktion des Telefons ist oder aber ob die Kreditkarte eine gefälschte Reproduktion unter Verwendung von gestohlenen Karten ist. In Abhängigkeit von vorgegebenen Befehlen wird, wenn das rechnergestützte Kontenführungssystem keine entgegengesetzten Anweisungen erhält, innerhalb von beispielsweise zwei oder drei Minuten das rechnergestützte Kontenführungssystem den Vorgang autorisieren. Wenn der wahre Eigentümer glaubt, daß der Vorgang unberechtigt ist, kann er sofort jede Form einer Kommunikationseinrichtung verwenden, etwa ein Telefon, um das jeweilige rechnergestützte Kontenführungssystem davon in Kenntnis zu setzen, daß der Vorgang widerrechtlich ist. Wenn dies der Fall ist, wird das rechnergestützte Kontenführungssystem ein vorgegebenes Signal zurück an den Verkaufsort oder aber die Bank senden, um der Einrichtung, an der der Vorgang stattfindet mitzuteilen, daß der Vorgang zurückzuweisen ist oder aber daß der Vorgang zu beenden ist. Das Signal

auf dem Bildschirm der die Kreditkarte lesenden Einrichtung am Ort des Verkaufs kann beispielsweise angeben, daß die Karte zurückgewiesen wird, oder aber das Signal, das den Betrieb des Mobiltelefons erlaubt, wird unterbrochen, um das Gespräch zu beenden. In diesem Fall können der wahre Eigentümer, die Bank, die Telefongesellschaft bzw. die Händler jeden Verlust aufgrund eines widerrechtlichen Vorgangs vermeiden oder jedenfalls reduzieren. Gewerbliche Vergehen dieser Art können so verringert werden. Der gesamte Vorgang kann etwa ein oder zwei Minuten oder aber auch weniger betragen.

Es wird jetzt auf Fig. 2 Bezug genommen. Es wird ein System gezeigt, das aufweist: eine Mehrzahl von Vorgangsvorrichtungen 1, eine Mehrzahl von entsprechenden rechnergestützten Kontenführungssystemen 2, eine oder mehrere Vorgangssignalübertragungsstationen 3, eine Mehrzahl von Kontenempfängern 4 und eine oder mehrere Übertragungseinrichtungen. Die Vorgangseinrichtungen 1 können, wie oben erwähnt, verschiedene Einrichtungen sein, etwa Kreditkarten lesende Einrichtungen, Mobiltelefone, Kassen oder dergleichen, die jeweils Einrichtungen zur unbaren, sofortigen Bezahlung sind. Die Vorgangseinrichtungen 1 erzeugen Vorgangssignale, wenn eine Transaktion stattfindet und senden das Vorgangssignal an das rechnergestützte Kontenführungssystem 2. Das rechnergestützte Kontenführungssystem 2 weist eine Zentralrecheneinheit (CPU) 2a, eine Ausgabeeinrichtung 2b und einen persönlichen Geheiminformationsspeicher 2c auf. Die CPU 2a wird verwendet, um die Vorgangsinformation aufzuzeichnen, die in dem Vorgangssignal von der Vorgangseinrichtung 1 empfangen wird. Wenn das rechnergestützte Kontenführungssystem beispielsweise ein Bankrechner ist, wird die Information stattfinden unter Verwendung der Kreditkarten, der Zeit und dem Datum der Transaktion, der Kartennummer oder, wenn die CPU ein Computer einer Telefongesellschaft ist, wird die Information die Nummer des Mobiltelefons, der Ort, an dem das Telefon ruft und die gewährte Telefonnummer, die Zeit und das Datum, die Zeitdauer des Anrufs usw. Die CPU 2a wird auf den persönlichen Adreßcode zurückgreifen, der in dem persönlichen Geheiminformationsspeicher 2c gespeichert ist, die von der Vorgangseinrichtung 1 angegebenen Signale verarbeiten und die Vorgangssignale einschließlich der Vorgangssignale an die Ausgabeeinrichtung 2b aussenden. Die Ausgabeeinrichtung 2b gibt sofort alle Informationssignale an, die Übertragungsstation 3 für die Vorgangssignale mittels einer drahtlosen Übertragung, des Telefonnetzes oder geeigneter Kommunikationskabel aus. Die Übertragungsstation 3 für das Vorgangssignal weist einen Codeeditor 3a, einen Programmcontroller 3b, einen aufnehmenden und persönlichen Adreßcodespeicher 3c und einen Übertrager 3b auf, der die ankommenden Informationssignale aufnimmt und prüft, ob der persönliche Geheimcode des wahren Eigentümers derselbe ist wie der persönliche Adreßcode in dem Speicher 3c, um diesen in dem codierten Editor 3a zu codieren. Der Programmcontroller 3b überträgt das Codesignal an den Übertrager 3d, der die codierte Vorgangsinformation unmittelbar in einen Bereich, in dem der wahre Eigentümer ist, überträgt, so daß der wahre Eigentümer die Vorgangsinformationssignale empfangen kann. Der wahre Eigentümer muß einen Kontenempfänger 4 zum Empfangen der Vorgangsinformation haben. Der Kontenempfänger 4 weist einen Empfänger 4a, einen Decoder 4b, eine Zentralrecheneinheit (CPU) 4g, einen Speicher mit wahlfreiem

Zugriff (RAM) 4c, eine Ansprecheinheit 4e, ein Display 4f und einen zur Identifikation dienenden Nurlesespeicher (ROM) 4d auf.

Der Empfänger 4a empfängt die codierten Vorgangsinformationssignale, die von der Übertragungsstation 3 für die Vorgangssignale übermittelt wird und sendet diese zu dem Decoder 4b. Der Decoder 4b bezieht sich auf den persönlichen Adreßcode des wahren Eigentümers in dem Identifikations-ROM 4d und codiert die Vorgangsinformationssignale und sendet diese Signale zu der CPU 4g. Die CPU 4g steuert die Programmanordnungen und startet die Ansprecheinheit 4e und das Display 4f und das RAM 4c. Die Ansprecheinheit 4e kann eine Toneinheit, eine Vibrationseinheit, eine Flüssigkeitskristallanzeige oder dergleichen aufweisen und wird dazu verwendet, den wahren Eigentümer von der Tatsache in Kenntnis zu setzen, daß ein ihn betreffender Vorgang stattfindet. Die Displayeinheit 4f zeigt die Information, die den Vorgang betrifft. Der Speicher 4c mit wahlfreiem Zugriff (RAM) ist ein Speicher, der dazu dient, die Vorgangsinformation zeitweise zu speichern. Wenn der wahre Eigentümer die Vorgangsinformation benötigt, kann er die Information, die in dem Speicher 4c gespeichert ist, verwenden. Wenn der wahre Eigentümer die Information nicht mehr benötigt, kann er Befehle eingeben, um die Information, die in dem Speicher 4c gespeichert ist, zu löschen.

Der wahre Eigentümer kann von dem Display 4f beurteilen, ob der Vorgang berechtigt oder nicht berechtigt ist. Wenn der Vorgang von dem wahren Eigentümer selbst veranlaßt ist, etwa einem Manager, der eine Kreditkarte der Firma verwendet, um eine Rechnung zum Einladen von Firmengästen für ein gemeinsames Essen zu zahlen, ist der Vorgang berechtigt. Der wahre Eigentümer der Kreditkarte benötigt keinen weiteren Vorgang. Der Vorgang wird autorisiert wie oben beschrieben und kann weitergehen. Wenn die auf dem Display 4f gezeigten Symbole den wahren Eigentümer wissen lassen, daß der Vorgang unberechtigt ist, etwa einen Vorgang, bei dem jemand das Mobiltelefon des Eigentümers verwendet, das dieser gerade zuvor verloren hat, oder aber wenn jemand eine gefälschte Kreditkarte mit gestohlener Information verwendet, um den Eigentümer zu veranlassen, eine Rechnung zu bezahlen, kann der wahre Eigentümer eine beliebige Kommunikations-einrichtung, etwa ein Telefon verwenden, um das entsprechende rechnergestützte Kontenführungssystem 2 zu informieren, den unberechtigten Vorgang zurückzuweisen oder zu stoppen. Das rechnergestützte Kontenführungssystem 2 wird entsprechend dieser Anordnung, bei der der wahre Eigentümer die Befehlssignale zum Zurückweisen oder zum Stoppen des Vorgangs an die Vorgangseinrichtung 1 sendet. Wenn, beispielsweise, die Vorgangseinrichtung 1 eine Einrichtung zum Lesen einer Kreditkarte ist durch Instruieren der Einrichtung, die Zahlung zurückzuweisen, oder aber durch Rückführen zu dem jeweils verwendeten Mobiltelefon und zum Unterbrechen des Gesprächs. Auf diese Weise können die Verluste des wahren Eigentümers der Kreditkarte und/oder des Mobiltelefons verringert werden, als auch die Verluste der Bank bzw. der Telefongesellschaft. Auf diese Weise können gewerbliche Vergehen unter unberechtigter Verwendung von unbaren sofortigen Zahlungstransaktionen verringert oder vermieden werden. Ein solches System hat einen großen Nutzen für die Gesellschaft und die Wirtschaft eines Landes.

Das rechnergestützte Kontenführungssystem 2 kann das vorhandene rechnergestützte Kontenführungssystem

sein, das von Banken oder Telefongesellschaften verwendet wird, mit einer zusätzlichen Ausgabeneinrichtung 2b. Die Ausgabeneinrichtung 2b wird verwendet, um die Vorgangsinformation für den wahren Eigentümer zu der Übertragungsstation für das Vorgangssignal zu übertragen. Die Übertragungsstation 3 für das Vorgangssignal kann ein üblicherweise verwendetes Pagingssystem oder eine andere Form einer Übertragungsstation sein. Der Kontenempfänger kann ein Pager, ein tragbarer Pager, ein Tabellenpager oder eine Uhr mit einer CPU 4g sein, eine sofortige Aufmerksamkeit bewirkende Einheit 4e und ein Display 4f zum Empfangen und zum Darstellen von einen Vorgang betreffenden Informationssignalen sein. Alternativ kann der Kontenempfänger ein Mobiltelefon, ein normales Telefon oder aber ein Computer oder eine besonders ausgebildete elektrische oder elektronische Einrichtung zum Empfangen und Darstellen von einen Vorgang betreffenden Informationssignalen und zum Bewirken der Aufmerksamkeit des wirklichen Eigentümers aufgrund der die Aufmerksamkeit bewirkenden Einheit 4e sein.

Fig. 3 zeigt zwei Beispiele von Kontenempfängern 4 und das jeweilige Identifikations-ROM 4d des Kontenempfängers 4. Der Kontenempfänger 4 weist einen persönlichen Identitätscode auf, der in dem Identifikations-ROM 4d von der Übertragungsstation 3 für das Vorgangssignal auf. Der Adreßcode ist demjenigen ähnlich, der dem verwendeten Pager gegeben ist, derart, daß der Pager von der Pagingstation selektiv identifizierbar ist. Mittels des Adreßcodes wird eine Botschaft von der Übertragungsstation 3 für das Vorgangssignal nicht durch jeden Kontenempfänger 4 empfangen werden, sondern nur von dem Kontenempfänger 4, der dem Kontenempfänger 4 der jeweiligen Person zugehörig ist. Der Adreßcode kann eine Zahl mit mehreren Stellen sein, etwa eine achtstellige Ziffer, eine zehnstellige Ziffer usw. Die Person, die den Kontenempfänger 4 trägt, muß den persönlichen Identitätsadreßcode nicht kennen. Der persönliche Identitätscode kann zuvor in das ID ROM 4d durch den Hersteller des Kontenempfängers eingeschrieben sein oder aber kann von der Übermittlungsstation für das Vorgangssignal eingeschrieben sein oder aber durch den Verwender, der manuell den Adreßcode ändert und dann die Übertragungsstation für das Vorgangssignal informiert. Allgemein ausgedrückt, ist wenigstens ein persönlicher Adreßcode in dem ID ROM 4d des Kontenempfängers 4 vorhanden, wie in Fig. 3-1 gezeigt. Der Kontenempfänger 4 muß dazu in der Lage sein, Vorgangssignale zu empfangen, beispielsweise Vorgangssignale verschiedener Kreditkarten, wenn die Ausgabeneinrichtung 2b des rechnergestützten Kontenführungssystems der Bank die Vorgangssignale übermittelt. Ein unterschiedlicher Code, der den wahren Eigentümer der Kreditkarte identifiziert, muß hinzugefügt sein. Wenn der Unterscheidungscode einer Person CB 12450 und das Vorgangssignal B 25 ist, wird das Display 4f des Kontenempfängers 4 die Symbole CB 12450 + B 25 angeben.

Der in Fig. 3-2 gezeigte Kontenempfänger kann Vorgangssignale von der Verwendung einer Kreditkarte empfangen. Die Bank, die die Kreditkarten ausgibt, kann in das Bankcomputersystem einen B-Adreßcode in den Identifikations-ROM 4d des Kontenempfängers einschreiben, der andere Kreditkarten unterscheiden kann. Für jede Kreditkarte schreibt die Bank einen B-Adreßcode für den wahren Eigentümer, d. h. den Kreditkarteneigentümer in das ID ROM des Kontenempfängers 4 ein. Auf dieselbe Weise verwendet die Telefonge-

sellschaft das rechnergestützte Schreibsystem 2 für jedes Mobiltelefon, um einen T-Adreßcode in das Identifikations-ROM 4d des Kontenempfängers 4 für den wahren Eigentümer einzuschreiben. Sodann wird in dem Kontenempfänger 4 wenigstens ein Identifikationscode durch die Übertragungsstation für das Vorgangssignal eingeschrieben, ein B-Adreßcode v n der jeweiligen Bank eingeschrieben und ein T-Adreßcode von der jeweiligen Telefongesellschaft eingeschrieben.

All diese Codes können natürlich von einem Pagermenü eingeschrieben werden, wenn der Kontenempfänger einen Pager verwendet. Üblicherweise sind zwei oder mehrere Adreßcode in dem Kontenempfänger 4 vorgesehen. Wenn der Vorgang stattfindet, wie in dem oben erwähnten Beispiel, wird das Display 4f des Kontenempfängers nur B 25 statt CB 12450 + B 25 anzeigen. Da der Adreßcode schon in den Kontenempfänger 4 eingeschrieben ist, kann das Symbol CB 12450 gespeichert werden und weitere den Vorgang betreffende Informationssymbole können auf dem Display 4f angezeigt werden. Dem wirklichen Eigentümer können so mehr Vorgangsinformationen wiedergegeben werden.

Fig. 4 zeigt ein dem in Fig. 2 gezeigten ähnliches Ausführungsbeispiel, bei dem eine Mehrzahl von Vorgangseinrichtungen jeweils einem entsprechenden rechnergestützten Schreibsystem zugehörig ist. Die Mehrzahl von rechnergestützten Schreibsystemen arbeiten dabei auf eine einzige Übertragungsstation 3 für die Vorgangssignale. Da die Übertragungsstation 3 für die Vorgangssignale mit einer Mehrzahl von rechnergestützten Kontenführungssystemen 2 verbunden ist, kann der Codeeditor 3a die Arbeitskapazität und die Geschwindigkeit der Vorgangsinformation erhöhen.

Der ganze Vorgang von dem Auftreten des Vorgangs zur Darstellung der Vorgangsinformation auf dem Kontenempfänger 4 benötigt nur Sekunden.

Fig. 5 zeigt ein anderes Ausführungsbeispiel der vorliegenden Erfindung, dem viele rechnergestützte Schreibsysteme durch auf entsprechende Anzahl von Übertragungsstationen 3 für das Vorgangssignal arbeiten, um eine Vorgangsinformation zu übertragen.

Die Vorgangsinformationssignale können unter den Übertragungsstationen für die Vorgangssignale derart übertragen werden, daß die Vorgangsinformationssignale über verschiedene Bereiche, verschiedene Regionen in einem Land oder verschiedenen Ländern oder auch über die Welt übertragen werden.

Fig. 6 zeigt ein anderes Ausführungsbeispiel der vorliegenden Erfindung, wobei eine Mehrzahl von rechnergestützten Computerschreibsystemen und eine Mehrzahl von Übertragungsstationen für das Vorgangssignal durch ein einziges rechnergestütztes Verarbeitungszentrum 3 für das Vorgangssignal miteinander verbunden sind, das eine große Anzahl von Vorgangsinformationen verarbeitet, die von allen rechnergestützten Kontenführungssystemen 2 kommen und daß die Signale unmittelbar an die richtigen Übertragungsstationen für das Vorgangssignal überträgt, um diese Information auszusenden.

Fig. 7 zeigt ein weiteres Ausführungsbeispiel der vorliegenden Erfindung, die eine Einheit 2f in dem rechnergestützten Kontenführungssystemen aufweist. Wenn der wahre Eigentümer angegeben hat, daß ein Vorgang unberechtigt ist und der Vorgang zurückgewiesen oder gestoppt wird, wird, bevor dieser Befehl an die Vorgangseinrichtung übermittelt wird, die die Polizei informierende Einheit aktiviert und informiert die Polizei darüber, daß ein unberechtigter Vorgang stattfindet und

wo der Ort dieses Vorgangs ist, so daß die Polizei unmittelbar eingreifen kann, um die Person, die unberechtigt agiert, festzunehmen.

Natürlich kann ein anspruchsvollerer Kontenempfänger 4 verwendet werden, der mehr Information beinhaltet, etwa welche Art von Transaktion ausgeführt wird, welche Karte verwendet wird, die Nummer der Kreditkarte, wieviel Geld bei der Transaktion ausgegeben wird, welche Art von Telefon verwendet wird, ob dies ein Mobiltelefon, ein Autotelefon, ein Zellulartelefon oder ein Telefon mit einer Geheimnummer ist, der Ort und die Zeit des Telefonanrufs, die angewählte Nummer und den Ort der Verwendung der Kreditkarte. Alle diese Informationen können durch Symbole, Worte oder Zeichen auf einem Display auf dem Kontoempfänger 4 angegeben werden. Auf diese Weise kann der wahre Eigentümer das erforderliche tun, um den Vorgang zu beenden.

Entsprechend schaffen das Verfahren und das Sicherheitssystem nach der vorliegenden Erfindung dem wahren Eigentümer der Kreditkarte oder des Mobiltelefons eine unmittelbare Kenntnis davon, daß eine Transaktion auftritt, so daß der wahre Eigentümer geeignetes unternehmen kann, wenn unbare sofortige Zahlungstransaktionen wie Zahlungen durch eine Kreditkarte, das Wählen mit einem Mobiltelefon oder dergleichen geschehen. Es versteht sich, daß dann, wenn eine unbare sofortige Zahlungstransaktion auftritt, daß entsprechende rechnergestützte Kontenführungssystem betrieben werden soll.

Das rechnergestützte Kontenführungssystem kann das Computersystem der Bank sein oder aber das Computersystem einer Dienstleistungsgesellschaft, etwa das Computersystem eines Dienstleisters für ein Zellulartelefon. All die obigen Computersysteme werden hier als "rechnergestützte Kontenführungssysteme" bezeichnet. Das rechnergestützte Kontenführungssystem soll Informationssignale ausgeben, die beinhalten, daß ein Vorgang (eine unbare sofortige Zahlungstransaktion) stattfindet und den in dem System aufgezeichneten persönlichen Adreßcode des wahren Eigentümers, die in dem System aufgezeichnet ist, an die Übermittlungsstation für das Vorgabesignal mittels eines Kommunikationsverfahrens, etwa einer drahtlosen Kommunikation, einer Übermittlungsinformation über das Telefonnetz oder ein geeignetes Kommunikationskabel. Die Übermittlungsstation für das Vorgangssignale sendet unmittelbar die Informationssignale für den Vorgang entsprechend ID-Code des wirklichen Eigentümers in der Station in dem geeigneten Gebiet aus. Der wahre Eigentümer kann schnell die Signale von einem Kontenempfänger aufnehmen, den er bei sich trägt, daß ein ihn betreffender Vorgang stattfindet. Entsprechend der empfangenen Signale kann der wirkliche Eigentümer beurteilen, ob er eine Maßnahme treffen muß oder nicht. Innerhalb eines vorgegebenen Zeitraums von etwa zwei bis drei Minuten wird dann, wenn der wahre Eigentümer nichts unternimmt, angenommen, daß der wahre Eigentümer mit dem Vorgang einverstanden ist und der Vorgang wird dadurch autorisiert. Sollte der wahre Eigentümer annehmen, daß der Vorgang eine illegale Verwendung einer gestohlenen Kreditkarte oder dergleichen ist, kann er ein beliebiges Kommunikationsmittel verwenden, um das entsprechende rechnergestützte Kontenführungssystem von der illegalen Verwendung in Kenntnis zu setzen. Ein rechnergestütztes Kontenführungssystem wird Signale an den Ort zurücksenden, an dem der Vorgang auftritt, etwa zurück zu der

Kreditkarte lesenden Einrichtung, um die Zahlung zu verweigern oder Signale können zu dem Mobiltelefon gesandt werden, um die Telefonverbindung zu unterbrechen. Die Verluste des wahren Eigentümers oder der betroffenen Dienstleistungsgesellschaft oder Bank werden verringert oder vermieden. Die gewerblichen Vergehen der Verwendung von gefälschten Kreditkarten oder gestohlenen Zellulartelefonen werden so verhindert.

Patentansprüche

1. Ein Sicherheitssystem zum Verhindern von unzulässigen Transaktionen, **gekennzeichnet durch:**

- eine Vorgangseinrichtung (1) zum Registrieren des Versuchs einer Transaktion; und
- Kommunikationsmittel (3) zum Inkennsetzen einer für eine solche Transaktion autorisierten Person von der versuchten Transaktion.

2. Ein Sicherheitssystem nach Anspruch 1, gekennzeichnet durch weitere Kommunikationsmittel (4), die es der berechtigten Person erlauben, die versuchte Transaktion zu autorisieren oder aber zu verhindern.

3. Ein Sicherheitssystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß ein rechnergestütztes Kontenführungssystem vorgesehen ist, wobei das rechnergestützte Kontenführungssystem in Kommunikation mit der Vorgangseinrichtung (1) ist, um Einzelheiten der versuchten Transaktion zu empfangen und betrieben werden kann, um weitere Einzelheiten der versuchten Transaktion an die autorisierte Person zu übermitteln.

4. Ein Sicherheitssystem nach einem der vorangehenden Ansprüche zur sofortigen Information des Berechtigten, daß ein unbarer, sofortiger Zahlungsvorgang, die ihn betrifft, stattfindet, gekennzeichnet durch:

- eine Vorgangseinrichtung (1); ein rechnergestütztes Kontenführungssystem (2); eine Übertragungsstation (3) für ein Vorgangssignal; und einen Kontenempfänger (4), wobei die Vorgangseinrichtung (1) eine Kreditkartenleseeinrichtung zum Lesen einer Kreditkarte, einer Mitgliedskarte, einer Clubkarte, einer magnetischen Karte, usw. aufweist, um eine Zahlung zu bewirken oder aber verschiedene Arten von mobilen Telefonen wie Zellulartelefonen, Autotelefonen, Geheimcodetelefonen usw., wenn ein Vorgang stattfindet, wobei die Vorgangseinrichtung (1) eine Vorgangsinformation erzeugt und die Vorgangsinformation einem entsprechenden rechnergestützten Kontenführungssystem (2) übermittelt, wobei das rechnergestützte Kontenführungssystem (2) die einkommenden Vorgangsinformationssignale von der Vorgangseinrichtung (1) verarbeitet, den persönlichen Adreßcode des wahren Besitzers mit dem Code in dem persönlichen Geheiminformationsspeicher vergleicht, diese Information der Übertragungsstation (3) für das Vorgangssignal übermittelt, die Übertragungsstation (3) für das Vorgangssignal einen Codeeditor (3a), einen Programmcontroller (3b), einen speichernden und persönlichen Adreßcodespeicher (3c) und einen Übermittler (3d) aufweist; der Codeeditor (3a) den persön-

lichen Adreßcode des wahren Berechtigten in dem Speicher- und persönlichen Adreßcodespeicher (3c) kombiniert, die empfangenen verschiedenen den Vorgang betreffenden Informationssignale codiert, der Programmcontroller (3b) den Übermittler (3d) unmittelbar dazu veranlaßt, die codierten Signale der den Vorgang betreffenden Informationssignale in Kombination mit dem persönlichen Adreßcode auszusenden, der Kontenempfänger (4) einen Empfänger, eine die Aufmerksamkeit bewirkenden Decoder (4b) mit einem RAM ID ROM, eine Displayeinheit (4f) und die CPU (4g) aufweist; der Empfänger die codierten Informationssignale, die sich auf den persönlichen Adreßcode, der von der Übermittlungsstation für das Vorgangssignal übersendet wird, empfängt und zu dem Decoder (4b) sendet, um durch die Steuerung der CPU (4g) zu decodieren, um die Aufmerksamkeitseinheit (4e) zu starten, um Töne, eine Vibration, ein Blinken von LCD oder dergleichen um die ankommende Information darzustellen, startet, und die Displayeinheit (4f), die den Vorgang betreffende Information mittels Symbolen, Ziffern, Worten oder Zeichen darstellt, und Speichern der den Vorgang betreffenden Information in dem RAM (4c) für eine spätere Verwendung.

5. Ein Sicherheitssystem nach Anspruch 4, dadurch gekennzeichnet, daß das rechnergestützte Kontenführungssystem (2) ein rechnergestütztes Kontenführungssystem (2) für Kreditkarten ist, das in einer Bank benutzt wird mit einer zusätzlichen Ausgabereinrichtung, oder aber ein rechnergestütztes Telefonkontensystem ist, das in einer Telefongesellschaft verwendet wird, mit einer zusätzlichen Ausgabereinrichtung.

6. Ein Sicherheitssystem nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß die das Vorgangssignal übertragene Station eine Pagingstation oder aber ein Pagingssystem ist.

7. Ein Sicherheitssystem nach Anspruch 4, 5 oder 6, dadurch gekennzeichnet, daß der Kontenempfänger (4) ein tragbarer Pager, ein Tafelpager, eine Uhr, ein mobiles Telefon, ein allgemeiner Telefonrechner oder aber eine besonders ausgebildete elektrische oder elektronische Einrichtung zur Aufnahme von einem Vorgang betreffenden Informationssignalen und der Anzeige der den Vorgang betreffenden Information ist und eine die Aufmerksamkeit bewirkende Einheit zum Aufmerksammachen des betroffenen wahren Besitzers aufweist.

8. Ein Sicherheitssystem nach einem der Ansprüche 4 oder 7, wobei das ID ROM des Kontenempfänger (4s) wenigstens einen persönlichen Adreßcode ID-Code hat, der von der Übertragungsstation (3) für das Vorgangssignal eingeschrieben ist und/oder weitere Adreßcode, wie ein T-Adreßcode, der von einer Telefongesellschaft eingeschrieben ist und/oder ein B-Adreßcode, der von einem rechnergestützten Kontenführungssystem (2) einer Bank eingeschrieben ist.

9. Ein Sicherheitssystem nach Anspruch 4, dadurch gekennzeichnet, daß die Übertragungsstation (3) für das Vorgangssignal unterschiedliche Anzeigesymbole für unterschiedliche Vorgänge aussendet, etwa "BK" betreffend eines Vorgangs unter Ver-

wendung einer Kreditkarte ein "ST" betreffend eines Vorgangs mit einem Zellulartelefon, "KT" betreffend einen Vorgang mit einem Telefon mit einem Geheimcode, Ziffern, die den Geldwert des Vorgangs betreffen und Symbolen und Ziffern und Worten und Zeichen, die den Ort des Vorgangs, die angerufene Telefonnummer und dergleichen betreffen. 5

10. Ein Sicherheitssystem nach Anspruch 4, dadurch gekennzeichnet, daß eine Vielzahl von rechnergestützten Kontenführungssystem (2)en vorgesehen sind, die in einem Netzwerk verbunden sein können, wodurch der Signalbereich, der durch die Übertragungsstation (3) für das Vorgangssignal ausgesendet wird, wie erforderlich gewählt werden kann. 15

11. Ein Sicherheitssystem nach Anspruch 4 oder 10, dadurch gekennzeichnet, daß das rechnergestützte Verarbeitungszentrum für das Vorgangssignal vorgesehen ist, um die Anzahl der den Vorgang betreffenden Signale zu vergrößern und die Verarbeitungsgeschwindigkeit zu erhöhen. 20

12. Ein Verfahren zum Verwenden eines elektrischen oder elektronischen Kommunikationssystem zum sofortigen Informieren des wahren Berechtigten, daß ein ihn betreffender unbarer Zahlungsvorgang stattfindet, gekennzeichnet durch die folgenden Schritte: Übermitteln einer den Vorgang betreffenden Information an den wahren Berechtigten während der Zeit des Vorgangs, Möglichen einer Entscheidung des wahren Berechtigten, ob der Vorgang autorisiert ist und Informieren der den Vorgang ausführenden Einrichtung von der Entscheidung des Berechtigten. 30

Hierzu 7 Seite(n) Zeichnungen

35

40

45

50

55

60

65

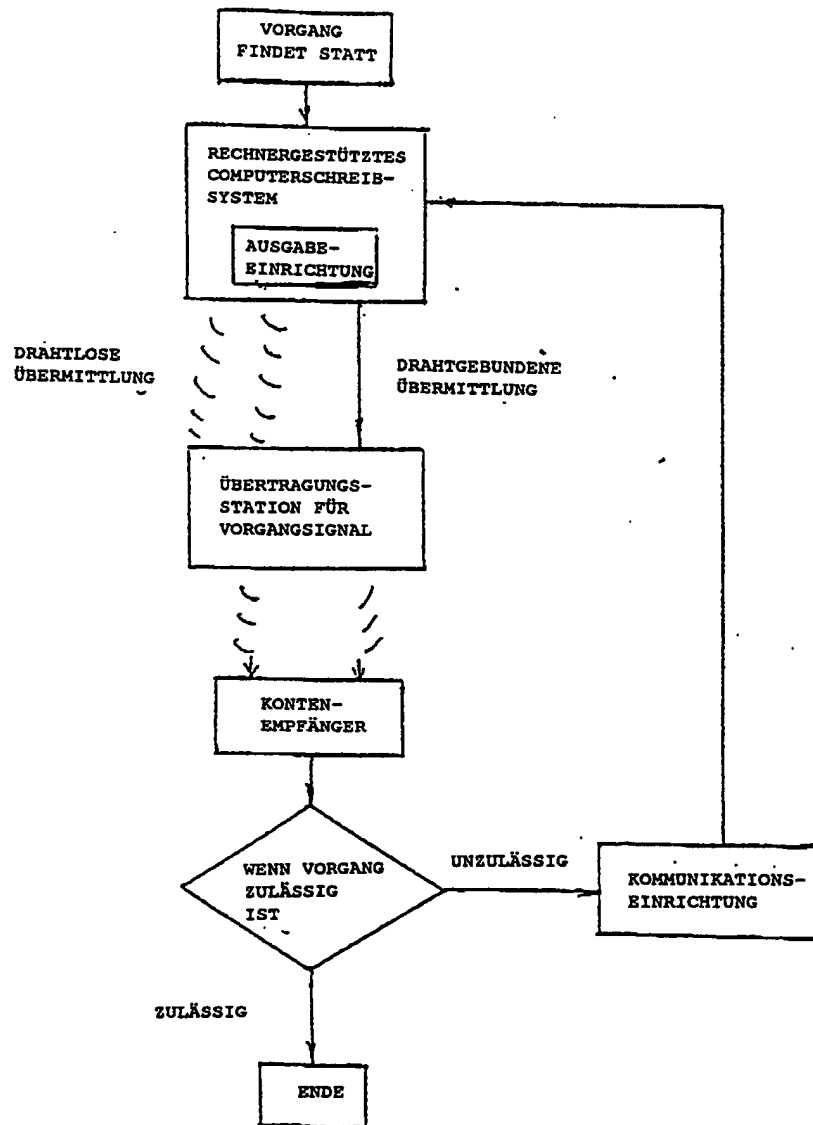


Fig.1

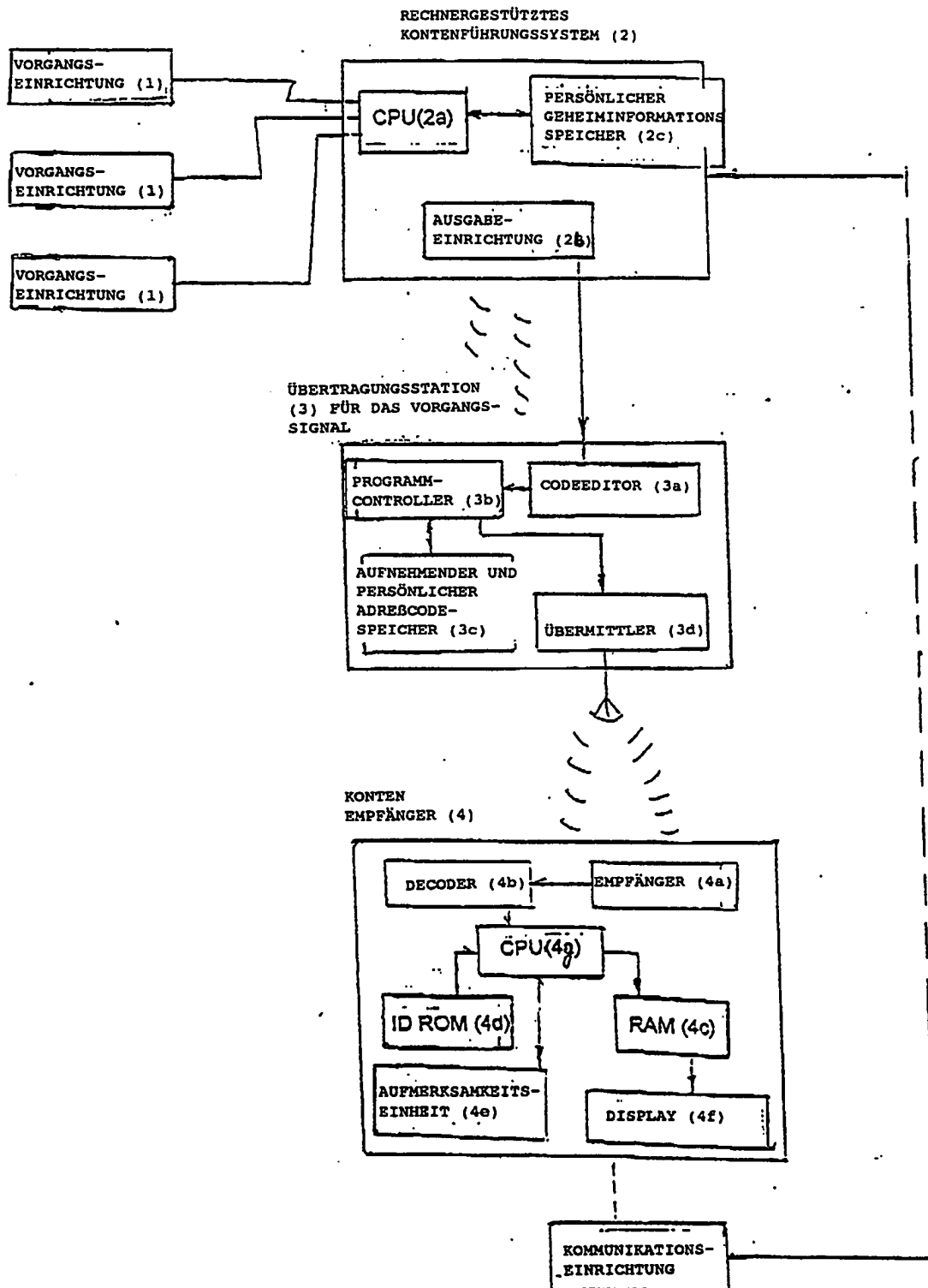
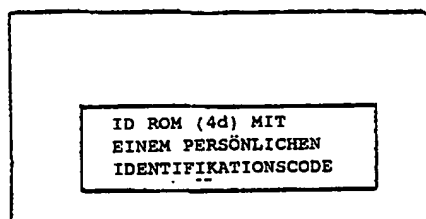


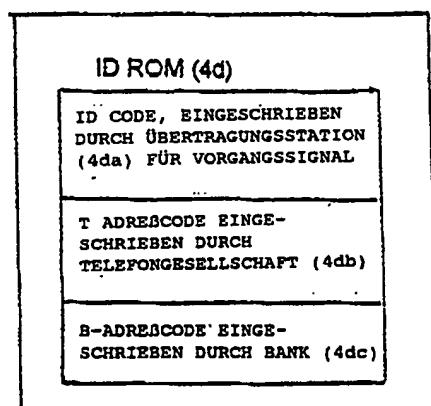
Fig.2

KONTENEMPFÄNGER (4)



(3-1)

KONTENEMPFÄNGER (4)



(3-2)

Fig.3

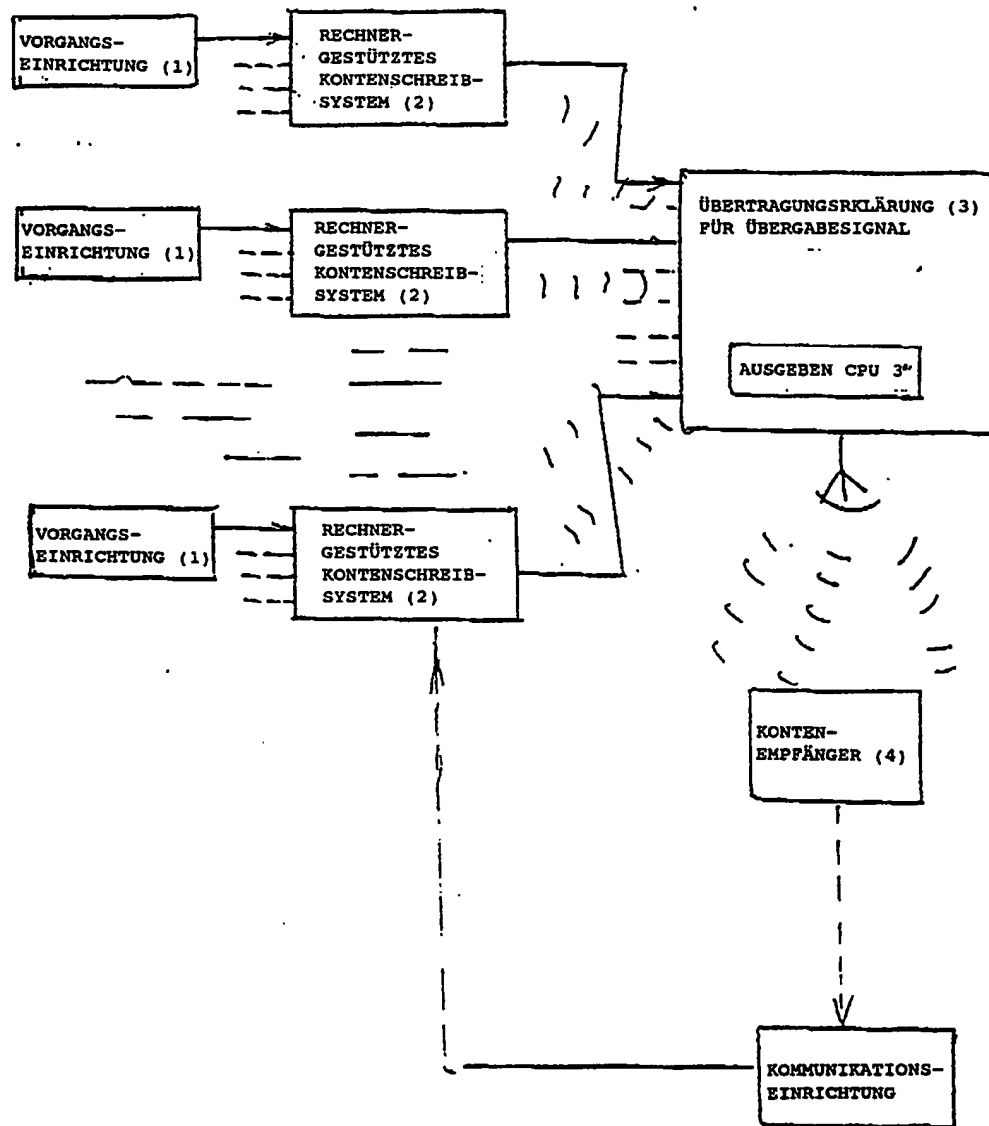


Fig.4

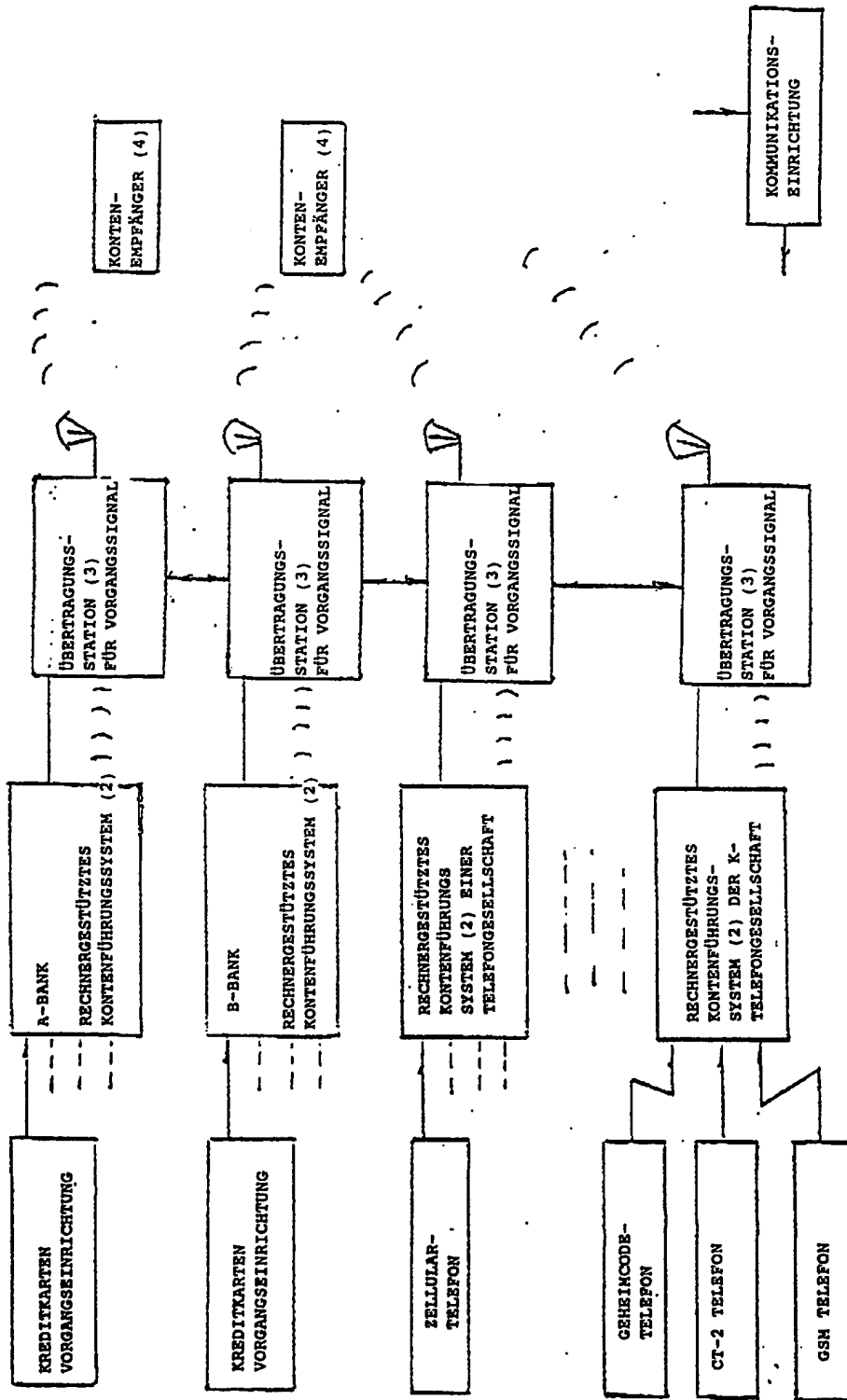


Fig.5

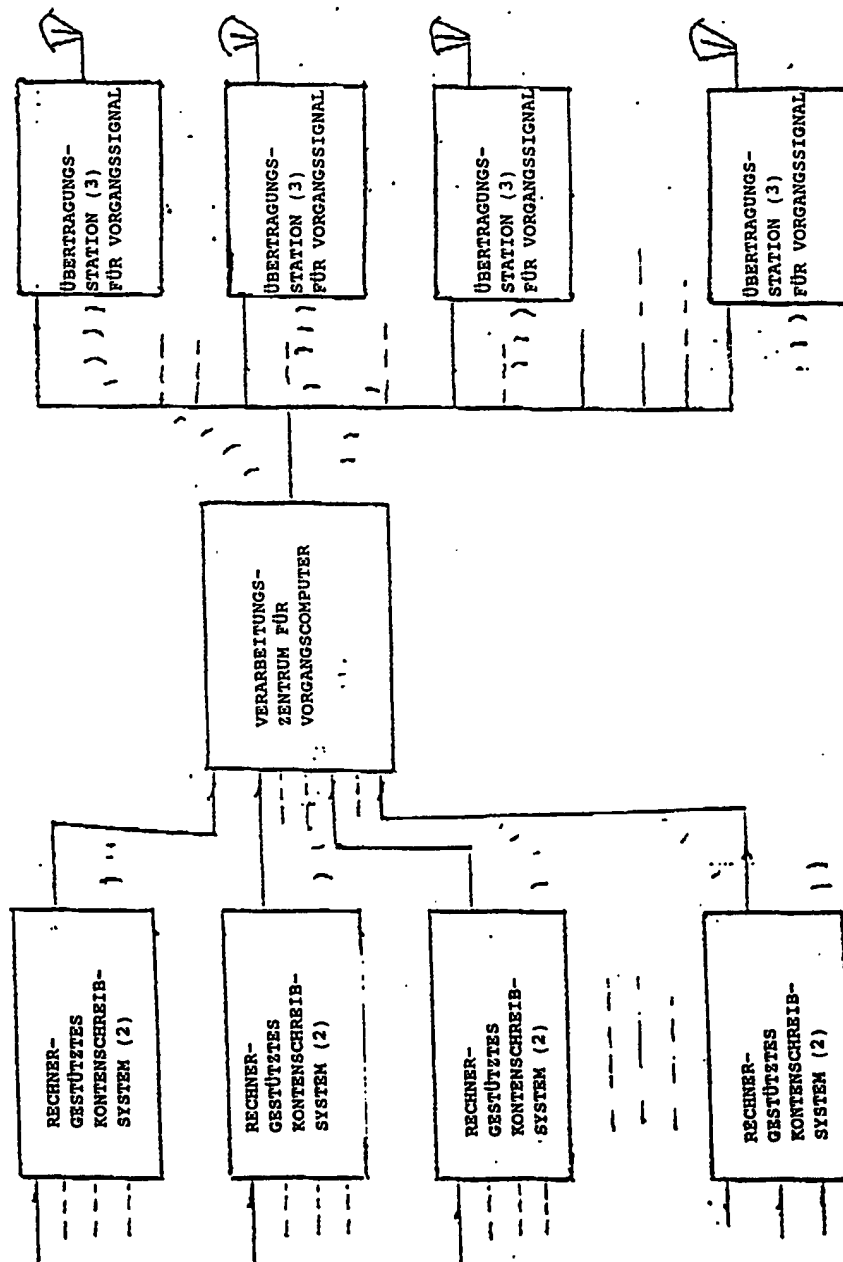


Fig. 8

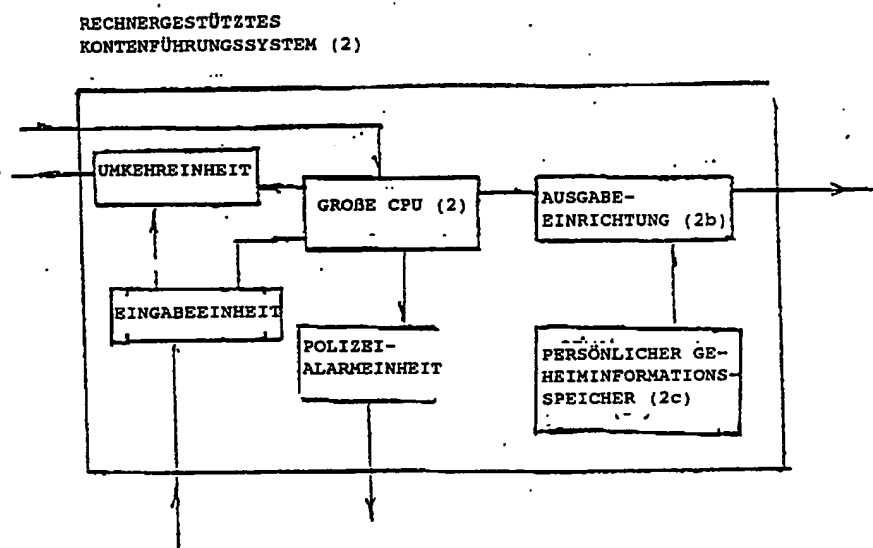


Fig.7